数理解析研究所講究録
1097巻 1999年 27-36

On unit equations

A Survey of Recent Developments of S-Unit Equations due to J.-H. Evertse, H.-P. Schlickewei and W. M. Schmidt

Noriko HIRATA-KOHNO

Department of Mathematics
College of Science and Technology
Nihon University
Suruga-dai, Kanda, Chiyoda, Tokyo 101-8308, Japan
email hirata@math.cst.nihon-u.ac.jp

代数的整数論のシンポジウムにて、昨年に続き、講演の機会を与えていただいたことに、深く感謝いたします。

ディオファントス問題と呼ばれる、不定方程式の数論的解の考察などの問題で、非常に大切な役割を持つもののひとつに、S-Unit Equation というものがあります。

ここでは、S-Unit Equation の最近の発展、特に J.-H. Evertse, H.-P. Schlickewei, W. M. Schmidt らによるこの数年間の進展を解説しました [E-Schl]。

1. Introduction

S-Unit Equation というものについて、まず簡単に復習する。

Kを $\mathbf{Q}$ 上有限次の代数体、$K^* = K - \{0\}$ とする。$a_1, \cdots, a_n \in K^*$に対し、$x_1, \cdots, x_n$を未知数とする方程式

$$a_1x_1 + \cdots + a_nx_n = 1 \tag{1}$$

を考える。ただし、

任意の non-empty subset I of $\{1 \cdots n\}$ に対して、その subsum は消えない、つまり

$$\sum_{i \in I} a_ix_i \neq 0 \tag{2}$$

という条件を常に満たすとする。

S を Kの place の有限集合で、無限素点をすべて含むものとし、固定する。S-単数とは、S のそとで単数となるものとする。未知数 $x_1, \cdots, x_n$を、K の単数群、あるいは S-単数群において考えるとき、この方程式 (1) を Unit Equation もしくは S-Unit Equation と呼ぶ。

S-Unit Equation (1) の解は有限であることが、$n = 2$ のときは Siegel によって示されている。これには、Roth の定理の少し弱い形である、Thue-Siegel の近似をもちいることは、昨年の筆者の講究録において解説してある。$n = 2$ のときの解の個数の評価は、J. H. Evertse によるものが Best known (1984, [E1]) で、その評価の数についても述べてあるが、s を Sの cardinality としたとき、3×7^{4s}以下、という評価であり、s 以外の何の情報にも依らない。たとえば、係数 a_1, a_2にも、Sの中身の places にもよらない。もちろん、$s \geq [K : \mathbf{Q}]/2$ なのだから、$[K : \mathbf{Q}]$ には依ることになる。また、$n > 2$ では open だが、$n = 2$ のときなら、Baker の方法で effective な解の評価がわかっている。

一般の n については、その有限性は W. M. Schmidt の Subspace Theorem から得られ、その解の個数の評価を初めて計算したのは、H. P. Schlickewei (1990, [Schl2]) である。その後この個数の評価は、改良され、一般の n についても、 Best known の記録をもっているのが、Evertse (1995,[E4])、その評価についても昨年の講究録に述べてある。

さて、本稿では、次のような考察を行う。

この S-Unit Equation (1) の解の有限性の証明の際、S-単数群の性質として用いられているのは、有限生成である、という事実なのである。したがって、S-単数群に限らず、K^*の有限生成なる乗法部分群 G に対しても、同じ性質が成り立つに違いないという、素朴な見方ができる。この洞察は実際正しく、Evertse (1984, [E2]) と、van der Poorten - H. P. Schlickewei (1991, [P-Schl]) の結果があり、証明にはやはり、Schmidt の Subspace Theorem を用いる。

このような素朴な洞察をさらに続けて、どのような場合に、(1) の形の方程式の解の有限性の証明が可能なのか、その必要十分条件の決定、とまではいかなくても、未知数の集合をできるだけ広く考えたい、という試みを行おう。また、係数についても、実際に代数的数であることを、どこまで使っているのか、群論的のような見方をしているとはいえないのか、など、あれこ

れ見直してみよう。

さらに、それぞれの場合で解の個数や、高さの評価が得られるならば、それが何に依っているのか、新しい dependence が得られないのか、などの問題に関し、以下、最近の結果について、順を追って紹介していく。

なお、ここで一応説明しておくが、何かが有限個である、としかわからない主張は、あまり説得力がない、という反論をかうことが多い。この場合、その有限集合の元が、explicit すなわち実際に全部書き下せるのならば、理想的であるのだが、そうもいかないとき、effective つまり理論的には、全部書き下すことが可能である、という主張が、望ましい。

しかし、それさえ言えない場合は、解の個数の上からの評価というのは、この有限個なる性質の、あいまいでない主張として役に立っているといえる。したがって、解の個数の上からの評価がわかっても、解を知ることは出来ないのだから意味がない、とはいえない。第一、解の個数なるものが、少なくとも何を用いて書けるのか、はっきりわかるだけでも、楽しいのであります。

2. Notations and results

K=$\mathbf{Q}$ 上有限次の代数体

$|\cdot|_\infty = |\cdot| = \mathbf{Q}$ の通常の絶対値

$|\cdot|_p$=$\mathbf{Q}$ の p-adic absolute value で 素数 p に対して $|p|_p = 1/p$ を満たすよう normalized されたもの

$M(K)$=$\{$places of K $\}$

$M^\infty(K)$=$\{$infinite places $\in M(K)\}$

$M_f(K)$=$\{$finite places $\in M(K)\}$

K_v=the completion of K at a place $v \in M(K)$ とおく。

$v \in M(K)$ に対して v が素数 p の上にあるとき $|x|_v = |x|_p$ for $x \in \mathbf{Q}$ となるよう絶対値 $|\cdot|_v$ を定める。

$\overline{\mathbf{Q}}$=$\mathbf{Q}$ の $\mathbf{C}$ 内の algebraic closure とし、

$v \in M(K)$ に対して $\|\cdot\|_v := |\cdot|_v^{d(v)}$ 但し $d(v) = \frac{[K_v:\mathbf{Q}_p]}{[K:\mathbf{Q}]}$ を K_vの algebraic closure $\overline{K_v}$ へ延長し、$\overline{K_v}$ 内への$\overline{\mathbf{Q}}$の埋め込みをを選んで固定してやれば、$\overline{\mathbf{Q}}$ 上の絶対値 $\|\cdot\|_v$が定まる。

さて、高さを定義する。$\mathbf{x} = (x_1 \cdots x_n) \in \overline{\mathbf{Q}}^n$をとる。

この $\mathbf{x}$ に対して、Kを $\mathbf{x} \in \mathbf{K^n}$なる代数体として一つとる。$v \in M(K)$ に

対して、 $\| \mathbf{x} \|_v = \max(\| x_1 \|_v \cdots \| x_n \|_v)$ とおき、$\mathbf{x}$ の高さを

$$H(\mathbf{x}) := \prod_{v \in M(K)} \| \mathbf{x} \|_v$$

と定義する。

Product Formula および Extension Formula から、Kのとりかたは関与しないことに注意する。

Sを infinite places 全部を含む、Kの place の有限集合とし、S整数の集合を

$O_S = \{x \in K : \| x \|_v \leq 1 \ \ for\ v \in M(K) - S\}$、$S$単数群を

$U_S = \{x \in K : \| x \|_v = 1\ for\ v \in M(K) - S\}$ とおく。

G=K^*の有限生成なる乗法部分群とする。$a_1, \cdots, a_n \in K^*$を係数、$x_1, \cdots, x_n \in G$ を未知数とする、(2) の条件を満たす方程式

$$a_1 x_1 + \cdots + a_n x_n = 1 \tag{3}$$

を考える。

G の free part のランクを r とおく。

Schlickewei は、Parametric subspace theorem (Quantitative version は 1996, [Schl 5]) というものを導入し、それにより、次の結果を得た。

定理 1 (Schlickewei, [Schl 7], to appear)

(3) の解は有限個で、個数は

$$2^{2^{26n}} \cdot 2^{16n^4 r + 4n^2 r^2} \cdot d^{6n^2(r+1)}$$

個以下である。ただし、$d = [K : \mathbf{Q}]$ である。

Evertse による Roth のレンマの改良 [E4] を用いて、Schlickewei は定理 1 の評価を改良し、その後、Schlickewei と Schmidt はさらに改良して

$$(2d)^{41n^3 r} r^{n^2 r}$$

を得た [Schl-Schm]。

ここで (3) の $n = 2$ のときを考える。Schlickewei は、(3) に対して、しばらく未解決予想であった、解の個数は n と rだけに依る、ということを証明した [Schl5]。しかも、G として、K^*に限らず、$\mathbf{C}^*$の有限生成乗法群（有限

r個の free part に、torsion の積も許す）であっても、よいという主張を示した。また、係数の範囲もひろげた。

具体的には次の評価となる。

定理 2 (Schlickewei [Schl8], to appear)

G を $\mathbf{C}^*$の有限生成乗法部分群、$n=2$ とする。また、$a_1, a_2 \in \mathbf{C}^*$とする。このとき、(3) の解の個数は

$$2^{2^{26}+9r^2}$$

個以下である。

これはその後、Schlickewei-Schmidt (to appear, [Schl-Schm]) により、$2^{14r+63}r^{2r}$ 個以下に改良された。また、F. Beukers-Schlickewei (1996, [Be-Schl]) は、hypergeometric functions を用いた方法で、$2^{16(r+1)}$という bound を得ている。E. Bombieri, J. Mueller, M. Poe らの、別の方法での bound も存在する (1997, [Bo-M-P])。

3. Absolute bound

ここでは、Schlickewei の Quantitative Parametric Subspace Thorem に対し、Evertse と Schlickewei が、代数体の Discriminant によらない評価を出したことと、その S-Unit Equation への応用について述べたい。

Kを $\mathbf{Q}$ 上 d 次の代数体とし、 Discriminant は D_Kであるとする。$v \in M(K)$ に対して、$\| \cdot \|_v$ を K_vまで延長しておく。今までと同じ、place の有限集合 S に対し、S^f を Sの finite places 全体、つまり $S{=}S^f \cup M^\infty(K)$ なるものとする。

$v \in S$に対し、$L_1^{(v)} \cdots L_n^{(v)}$ を K_v係数の linearly independent linear forms in $X_1 \cdots X_n$とおく。 $Q \geq 1$ を実数とし、$\mathbf{c} = (c_{iv} : v \in S,\ i = 1 \cdots n)$ を実数の組とし、

$$\Pi(Q, \mathbf{c}) = \{\mathbf{x} \in O_S^n : \| L_i^{(v)}(\mathbf{x}) \|_v \leq Q^{c_{iv}}$$

但し $v \in S, i = 1 \cdots n$ とおく。

実数$\lambda > 0$ に対して、

$\lambda\Pi(Q, \mathbf{c}) := \{\mathbf{x} \in O_S^n :$

$\| L_i^{(v)}(\mathbf{x}) \|_v \leq \lambda^{d(v)} Q^{c_{iv}}$ $(v \in M^\infty(K), i = 1 \cdots n)$,

$\| L_i^{(v)}(\mathbf{x}) \|_v \leq Q^{c_{iv}}$ $(v \in S^f,\ i = 1, \cdots, n)\}$,
ただし $d(v) = 1/d$ if $K_v = \mathbf{R}$, $d(v) = 2/d$ if $K_v = \mathbf{C}$ とする。
The i-th successive minimum $\lambda_i = \lambda_i(Q, \mathbf{c})$ of $\Pi(Q, \mathbf{c})$ とは、 $\lambda\Pi(Q, \mathbf{c})$ が i 個の linearly independent vectors を含むようなすべての$\lambda > 0$ の下限として定義される。

$$\Delta = \prod_{v \in S} \| \det(L_1^{(v)} \cdots L_n^{(v)}) \|_v$$

$$\delta = -\Big(\sum_{v \in S} \sum_{i=1}^{n} c_{iv} \Big)$$

とおく。

さて、次に述べる結果は、D. Roy -J. Thunder(1996, [R-Th1]) によるものである。Fを Kの finite extension とし、S_F を、places of F で Sの上にあるもの全体とする。O_{S_F}は O_Sの integral closure in Fである。各 $v \in S$、$w \in S_F, w|v$ に対し、linear forms $L_i^{(w)}$ と実数 c_{iw} を次のように定める。

$$L_i^{(w)} = L_i^{(v)}, \qquad c_{iw} = d(w|v) \cdot c_{iv} \quad (i = 1 \cdots n)$$

但し $d(w|v) = \frac{[F_w : K_v]}{[F:K]}$である。

$$\Pi_F(Q, \mathbf{c}) = \{\mathbf{x} \in O_{S_F}^n : \| L_i^{(w)}(\mathbf{x}) \|_w \leq Q^{c_{iw}}$$

ただし $w \in S_F$, $i = 1 \cdots n$ と定める。さて、Kの finite extensions F, E で $F \subseteq E$なるものについては、$\Pi_E(Q, \mathbf{c}) \cap F^n = \Pi_F(Q, \mathbf{c})$ である。ここで、$\Pi(Q, \mathbf{c})$ の algebraic closure を

$$\overline{\Pi}(Q, \mathbf{c}) = \bigcup_{F \supseteq K} \Pi_F(Q, \mathbf{c})$$

と定義する。

Kのすべての finite extension Fと、実数$\lambda > 0$ に対して、
$\lambda\Pi(Q, \mathbf{c}) = \{\mathbf{x} \in O_S^n :$
$\| L_i^{(w)}(\mathbf{x}) \|_w \leq \lambda^{d(w)} Q^{c_{iw}} (w \in M^\infty(K), i = 1, \cdots n)$
$\| L_i^{(w)}(\mathbf{x}) \|_w \leq Q^{c_{iw}} \} (w \in S_F^f, i = 1, \cdots n)\}$,
ただし $d(w) = \frac{1}{[F:\mathbf{Q}]}$ if $F_w = \mathbf{R}$, $d(w) = \frac{2}{[F:\mathbf{Q}]}$ if $F_w = \mathbf{C}$ とする。

さて$\overline{\Pi}(Q,\mathbf{c})$の$i$-th successive minimum $\overline{\lambda}_i = \overline{\lambda}_i(Q,\mathbf{c})$ とは、$\lambda\overline{\Pi}(Q,\mathbf{c})$が、$i$個の linearly independent vectors from $\overline{O_S}^n$を含むような、すべての$\lambda > 0$の下限として定義される。

定理3 (Roy -Thunder, 1996 [R-Th1])

$\overline{\Pi}(Q,\mathbf{c})$はちょうど$n$個のsuccessive minimumで、次を満たすものをもつ。
$0 < \overline{\lambda}_1 \leq \cdots \leq \overline{\lambda}_n < \infty$ かつ、

$$n^{-n/2}\Delta Q^\delta \leq \overline{\lambda}_1 \cdots \overline{\lambda}_n \leq e^{n(n-1)/4}\Delta Q^\delta$$

この、どこにもDiscriminantの登場しないsuccessive minimumの存在定理を用いると、次の定理4が証明できる。

K, Sは上述のものとし、$L_i^{(v)}$ $(v \in S,\ i = 1 \cdots n)$ を linear forms で以下の性質を満たすものとする。
Hは正数とする。
$v \in S$に対し、$\{L_1^{(v)} \cdots L_n^{(v)}\}$ はK係数、変数が$X_1 \cdots X_n$の linearly independent なる一次形式であり、$L_i^{(v)}$の係数ベクトルの高さ$H(L_i^{(v)})$について、$H(L_i^{(v)}) \leq H$, $\| L_i^{(v)} \|_v = 1$ for $v \in S$, $i = 1 \cdots n$ が満たされ、さらに、$\{L_1^{(v)} \cdots L_n^{(v)}\}$ $(v \in S)$ のなかに、ちょうどR個の異なる集合があるとする。加えて、$\mathbf{c} = (c_{iv} : v \in S,\ i = 1 \cdots n)$ を実数の組としたとき、

$$\sum_{v \in S} \sum_{i=1}^{n} c_{iv} \leq -\delta$$

ただし$0 < \delta \leq 1$、

$$\sum_{v \in S} \max(c_{1v} \cdots c_{nv}) \leq 1$$

が成り立っているとする。今

$$\Delta = \prod_{v \in S} \| \det(L_1^{(v)} \cdots L_n^{(v)}) \|_v$$

とおく。

0.3cm

定理 4 (Evertse-Schlickewei, to appear [E-Schl])

$$b \leq 4^{(n+5)^2}\delta^{-n-3}\log 4R \cdot \log(\delta^{-1}\log 4R)$$

なる、$\overline{\mathbf{Q}}^n$ の proper linear subspaces $T_1 \cdots T_b$ で、次を満たすものが存在する。

$$Q \geq \max\left(H,\ (n^{n/2}\Delta^{-1})^{2/\delta}\right)$$

を満たす全ての Q に対して、

$$\overline{\Pi}(Q, \mathbf{c}) \subset T_i$$

なる $i \in \{1 \cdots b\}$ が存在する。

そして、この定理 4 から、次の定理 5 が示せる。

定理 5 (Evertse-Schlickewei-Schmidt, to appear [E-Schl-Schm])

G として $\mathbf{C}^*$ のランク r の有限生成乗法群とする。$a_1 \cdots a_n \in \mathbf{C}^*$ をとる。このとき、(2) を満たす (3) の解は、高々

$$c(n)^{r+2}$$

個である。ただし、
$c(n) = \exp\left((6n)^{4n}\right)$。

つまりここで、(2) を満たす (3) の解の個数は、n と r のみを用いて表され、それ以外には、d を用いる必要のないことが証明された。

References

[Be-Schl] Beukers, F., Schlickewei, H.P., The equation $x+y=1$ in finitely generated groups. Acta Arith. 78 (1996), 189–199

[Bo-M-P] Bombieri E., Mueller, J., Poe, M., The unit equation and the cluster principle. Acta Arith. 79 (1997), 361–389

[E1] Evertse, J.-H., On equations in S-units and the Thue-Mahler equation. Invent. Math. 75 (1984), 561–584

[E2] — On sums of S-units and linear recurrences, Compos. Math. 53 (1984), 225–244

[E3] — The number of solutions of decomposable form equations, Invent. Math. 122 (1995), 559–601

[E4] — An explicit version of Faltings' Product Theorem and an improvement of Roth's lemma. Acta Arith. 73 (1995), 215–248

[E5] — An improvement of the quantitative Subspace theorem. Compos. Math. 101 (1996), 225–311

[E6] — The number of solutions of linear equations in roots of unity. In preparation.

[E-Schl] Evertse, J.-H., Schlickewei, H.P., A quantitative version of the absolute Subspace theorem. In preparation.

[E-Schl-Schm] Evertse, J.-H., Schlickewei, H.P., Schmidt, W.M., Linear equations with variables which lie in a multiplicative group. In preparation.

[Mc] McFeat, R.B., Geometry of numbers in adele spaces. Dissertationes Mathematicae 88, PWN Polish Scientific Publishers, Warsaw 1971

[P-Schl] Poorten, A.J. van der, Schlickewei, H.P., Additive relations in fields. J. Austral. Math. Soc. (Ser. A) 51 (1991), 154–170

[R-Th1] Roy, D., Thunder, J.L., An absolute Siegel's Lemma. J. reine angew. Math. 476 (1996), 1–26

[R-Th2] — A note about Siegel's Lemma on the algebraic closure of a global field. Preprint.

[Schl1] Schlickewei, H.P., The $\wp$-adic Thue-Siegel-Roth-Schmidt theorem. Arch. Math. 29 (1977), 267–270

[Schl2] — S-unit equations over number fields. Invent. Math. 102 (1990), 95–107

[Schl3] — The quantitative Subspace Theorem for number fields. Compos. Math. 82 (1992), 245–274

[Schl4] — Equations in roots of unity. Acta Arith. 76 (1996), 99-108

[Schl5] — Multiplicities of recurrence sequences. Acta Math. 176 (1996), 171–243

[Schl6] — The multiplicity of binary recurrences. Invent. Math. 129 (1997), 11–36

[Schl7] — Linear equations over finitely generated groups. Annals of Math., to appear

[Schl8] — Equations $ax + by = 1$. Annals of Math., to appear

[Schl9] — A parametric version of the Subspace theorem. Preprint.

[Schl-Schm] Schlickewei, H.P., Schmidt, W.M., Linear equations with variables which lie in a multiplicative group. Preprint.

[Schm1] Schmidt, W.M., Norm form equations. Annals of Math. 96 (1972), 526–551

[Schm2] — The subspace theorem in diophantine approximations. Compos. Math. 69 (1989), 121–173

[Schm3] — Heights of Algebraic Points Lying on Curves or Hypersurfaces. Proc. A.M.S. 124 (1996), 3003–3013

[Schm4] — Heights of points on subvarieties of $\mathbf{G}_m^n$. In: Séminaire de théorie des nombres de Paris, 1993–1994 (ed. by S. David), 157–187. Cambridge Un. Press, 1996

[Z1] Zhang, S., Positive line bundles on arithmetic surfaces. Annals of Math. 136 (1992), 569–587

[Z2] — Positive line bundles on arithmetic varieties. Journal A.M.S. 8 (1995), 187–221